COMMUNIQUE DE PRESSE NATIONAL – PARIS – 21 JUIN 2022

Présentation de la stratégie nationale cyber : 7 projets retenus dans le cadre du Programme et équipement prioritaire de recherche

Piloté par le CNRS, Inria et le CEA, le programme et équipement prioritaire de recherche (PEPR) Cybersécurité vise à renforcer l'excellence de la recherche française et soutenir le développement de la filière cybersécurité. Lancé ce 21 juin 2022, il s'inscrit dans une stratégie nationale d'accélération annoncée par le Président de la République le 21 février 2021, dont il constitue le volet recherche amont. Doté d'un budget de 65 millions d'euros sur 6 ans, financé dans le cadre du PIA 4 (devenu France Relance), il vient de présenter 7 premiers projets de recherche ciblés.

Dans un contexte d'une menace cyber en constant développement et d'une grande compétition mondiale visant le développement de solutions pour protéger les citoyens, les acteurs économiques et institutionnels, la France s'est dotée d'une Stratégie nationale Cybersécurité, dans le cadre du PIA4. Le but : tripler le chiffre d'affaires de la filière d'ici 2025, former plus de professionnels et développer des solutions souveraines alors que l'enjeu de cybersécurité est devenu encore plus visible lors de la crise sanitaire, par l'amplification du télétravail, et les cyberattaques contre les opérateurs d'importance vitale et les institutions, rapportées par l'ANSSI dans son dernier Panorama de la menace cyber.

Soutenant des activités de recherche au meilleur niveau mondial, le PEPR Cybersécurité renforcera l'effort national en la matière et ses résultats nourriront les actions plus aval de cette stratégie, telles que le programme de transfert du Campus Cyber opéré par Inria ainsi que le prototypage de solutions souveraines dans les appels à projets. Impliquant environ 200 chercheurs et enseignants-chercheurs permanents issus du CNRS, du CEA, d'Inria, ainsi que de 22 universités[1] et grandes écoles[2], il fait appel à plusieurs disciplines : informatique, mathématiques, électronique et traitement du signal pour aider à sécuriser les trois couches du cyberespace (matériel, logiciel, données).

Le PEPR soutient des actions spécifiques avec notamment la mise en place de projets ciblés. Des actions d'animation et de transferts de connaissance entre académiques et industriels seront également mis en place.

Sept premiers grands projets ciblés portant sur deux axes ont été mis sur pied. Un appel à projet, lancé en juin et opéré par l'ANR, permettra de financer trois projets additionnels.

Les 7 premiers projets ciblés

Axe Sécurité de l'information

Le projet **iPOP** (Projet interdisciplinaire sur la protection des données personnelles) vise à étudier les menaces vis-à-vis de la vie privée introduites par ces nouveaux services et de concevoir des solutions théoriques et techniques de protection de la vie privée, compatibles avec la réglementation française et européenne, qui préservent la qualité d'expérience des utilisateurs. Ces solutions seront déployées et évaluées, à la fois sur leurs aspects technologiques, mais également juridiques et d'acceptabilité sociétale.

Le projet **SECURE COMPUTE** (Sécurité des calculs) vise à étudier les mécanismes cryptographiques permettant d'assurer la sécurité des données, au cours de leur transfert ainsi que pendant toute la période de stockage, mais également lors de traitements, malgré des environnements non-maîtrisés tels qu'Internet pour les échanges et le Cloud pour l'hébergement et le traitement.

Le projet **SVP** (Vérification de protocoles de sécurité) vise à permettre l'analyse de protocoles déployés ou en cours de déploiement, aussi bien au niveau des spécifications de ces protocoles, que de leurs implémentations. Il développera des techniques et des outils permettant la mise en place de solutions dont la sécurité ne sera plus remise en question de manière cyclique.

Le projet **DEFMAL** (Défense contre les programmes Malveillants) vise l'étude des logiciels/programmes malveillants (malware, ransomware, botnet, etc). Il développera de nouvelles approches pour analyser les programmes malveillants et aidera à la compréhension globale de l'écosystème du malware dans une approche interdisciplinaire impliquant l'ensemble des acteurs concernés.

Axe Sécurité des systèmes

Le projet **SUPERVIZ** (Supervision et orchestration de la sécurité) cible la détection, la réponse et la remédiation aux attaques informatiques, sujets regroupés sous l'appellation de « supervision de sécurité », qui cherche à renforcer les mécanismes de protection préventifs et à pallier leurs insuffisances.

Le projet **SECUREVAL** vise à concevoir de nouveaux outils bénéficiant des nouvelles technologies numériques pour vérifier l'absence de vulnérabilités matérielles comme logicielles, et réaliser les preuves de conformité requises.

Le projet **ARSENE** vise à accélérer de manière coordonnée et structurée la recherche et le développement de solutions de sécurité souveraines et industrialisables. La mise en œuvre de démonstrateurs ASIC et FPGA intégrant les briques étudiées et développées permettra dans une dernière étape de tester et valoriser ces travaux de recherche.

Notes

1. Sorbonne Université ; Université Bretagne Occidentale ; Université Bretagne Sud ; Université de Lille ; Université de Lorraine ; Université de Montpellier ; Université de Rennes 1 ; Université de Versailles Saint-Quentin-en-Yvelines ; Université Grenoble Alpes ; Université Jean Monnet St Etienne ; Université Paris-Saclay.

2. ENS Rennes ; ENSTA Bretagne ; ENS PSL ; EURECOM ; Grenoble INP ; INSA CVL ; INSA Lyon ; INSA Rennes ; Institut Mines Télécom ; CentraleSupélec ; EDHEC.

Contacts

Presse CNRS I Priscilla Dacher I **T +33 1 44 96 46 06** I priscilla.dacher@cnrs.fr
Presse CEA I Tuline Laeser I **T +33 06 12 04 40 22** I tuline.laeser@cea.fr
Presse Inria I I Laurence Goussu I **T +33 1 39 63 57 29** I laurence.goussu@inria.fr